WHAT IS CLAIMED IS:

1. A method of encrypting a shared document, comprising:

under control of an encryption server system,

generating a ECC public/private key pair for the encryption server system;

under control of a client system,

requesting a Java® encryption applet from the encryption server system;

requesting an encryption server system EEC public key from the encryption server system;

under the control of the encryption server system,

transmitting the Java® encryption applet to the client system over a secure channel;

transmitting the encryption server system EEC public key to the client system over a secure channel;

under control of a client system,

receiving the Java® encryption applet from the encryption server system over a secure channel;

receiving the encryption server system EEC public key from the encryption server system over a secure channel;

installing the Java® encryption applet on the client system;

running the Java® encryption applet on the client system to generate a Triple DES symmetric key;

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

creating a relationship between the cipher text document and the Triple DES symmetric key;

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key;

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key;

transmitting the cipher text document to the encryption server system;

transmitting the encrypted Triple DES symmetric key to the encryption server system;

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system;

under the control of the encryption server system,

storing the cipher text document in a storage medium;

storing the encrypted Triple DES symmetric key in a storage medium; and

storing the relationship between the cipher text document and the encrypted Triple DES symmetric key in a storage medium.

2. The method of claim 1, wherein the secure channel is an SSL channel.

3. The method of claim 1, wherein the Java® encryption applet is installed on a browser.

4. The method of claim 3, wherein the browser is the Internet Explorer® or the Netscape Navigator®.

5. The method of claim 1, wherein the cipher text document is transmitted from the client system to the encryption server system using FTP, and the encrypted Triple DES symmetric key is transmitted to the encryption server system via HTTP.

6. The method of claim 1, wherein the cipher text document is transmitted from the client system to the encryption server system using FTP, and the document is decrypted upon arrival at the server.

7. The method of claim 1, further comprising the steps of:

under the control of the encryption server system,

storing the relationship between the cipher text document and the encrypted Triple DES symmetric key by making a first and a second entry in a correlation table, the first entry representing the encrypted Triple DES symmetric key, and the second entry representing the cipher text document.

8. The method of claim 7, wherein the first entry is the encrypted Triple DES symmetric key and the second entry is the cipher text document.

9. The method of claim 7, wherein the first entry is a pointer to the encrypted Triple DES symmetric key and the second entry is a pointer to the cipher text document.

10. The method of claim 1, further comprising the steps of:

under the control of the encryption server system,

decrypting the encrypted Triple DES symmetric key with the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

decrypting the cipher text document with the decrypted Triple DES symmetric key, thereby creating a clear text document; and,

storing the clear text document on the encryption server system.

11. The method of claim 7, further comprising the steps of:

under the control of the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;

decrypting the encrypted Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

decrypting the cipher text document with the decrypted Triple DES symmetric key, thereby creating a clear text document;

storing the clear text document on a storage medium; and

making a third entry in the correlation table, thereby creating a relationship between the cipher text document, the clear text document and the encrypted Triple DES symmetric key.

12. The method of claim 11, wherein the third entry is the clear text document.

13. The method of claim 11, wherein the third entry is a pointer to the clear text document.

14. The method of claim 7, further comprising the steps of:

under control of the client system,

requesting the cipher text document from the server;

under control of the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

15. The method of claim 14, wherein the Java® decryption applet is installed on a browser.

16. The method of claim 15, wherein the browser is the Internet Explorer® or the Netscape Navigator®.

17. The method of claim 10, further comprising the steps of:

under control of the client system,

requesting the clear text document from the server;

under control of the encryption server system,

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

18. The method of claim 17, wherein the Java® decryption applet is installed on a browser.

19. The method of claim 18, wherein the browser is the Internet Explorer® or the Netscape Navigator®.

20. The method of claim 11, further comprising the steps of:

under control of the client system,

requesting the clear text document from the server;

under control of the encryption server system,

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

21. The method of claim 20, wherein the Java® decryption applet is installed on a browser.

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key;

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key;

transmitting the cipher text document to the encryption server system;

transmitting the encrypted Triple DES symmetric key to the encryption server system;

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system;

under the control of the encryption server system,

storing the cipher text document in a storage medium;

storing the encrypted Triple DES symmetric key in a storage medium; and

storing the relationship between the document and the Triple DES symmetric key in a storage medium.

25. An encryption system for shared documents, comprising:

an encryption server system and a client system;

the encryption server system,

generating a ECC public/private key pair for the encryption server system;

transmitting the Java® encryption applet to the client system over a secure channel;

transmitting the encryption server system EEC public key to the client system over a secure channel;

storing the encrypted document in a storage medium;

storing the encrypted Triple DES symmetric key in a storage medium;

storing the relationship created between the document and the Triple DES symmetric key in a storage medium;

a client system,

requesting a Java® encryption applet from the encryption server system;

22. The method of claim 21, wherein the browser is the Internet Explorer® or the Netscape Navigator®.

23. The method of claim 1, further comprising the steps of:

under the control of the encryption server system,

decrypting the encrypted Triple DES symmetric key with the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key; and,

decrypting the cipher text document with the decrypted Triple DES symmetric key, thereby creating a clear text document.

24. A method of encrypting a shared document, comprising:

under control of a client system,

requesting a Java® encryption applet from the encryption server system;

requesting an encryption server system EEC public key from the encryption server system;

under the control of the encryption server system,

transmitting the Java® encryption applet to the client system over a secure channel;

transmitting the encryption server system EEC public key to the client system over a secure channel;

under control of a client system,

receiving the Java® encryption applet from the encryption server system over a secure channel;

receiving the encryption server system EEC public key from the encryption server system over a secure channel;

installing the Java® encryption applet on the client system;

running the Java® encryption applet on the client system to generate a Triple DES symmetric key;

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

creating a relationship between the cipher text document and the Triple DES symmetric key;

requesting an encryption server system EEC public key from the encryption server system;

receiving the Java® encryption applet from encryption server system over a secure channel;

receiving the encryption server system EEC public key from encryption server system over a secure channel;

installing the Java® encryption applet on the client system;

running the Java® encryption applet on the client system to generate a Triple DES symmetric key;

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

creating a relationship between the cipher text document and the Triple DES symmetric key;

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key;

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key;

transmitting the cipher text document to the encryption server system;

transmitting the encrypted Triple DES symmetric key to the encryption server system;

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system.

26. The encryption system of claim 25, wherein the encryption server system is further comprised of:

storing the relationship between the cipher text document and the encrypted Triple DES symmetric key by making a first and second entry in a correlation table, the first entry represents the encrypted Triple DES symmetric key, and the second entry represents the cipher text document.

27. The encryption system of claim 26, wherein the encryption server system is further comprised of:

making a third entry in the correlation table, wherein the third entry represents the clear text document;

creating a relationship between the cipher text document, the encrypted Triple DES symmetric key, and the clear text document; and,

storing the relationship between the cipher text document, the encrypted Triple DES symmetric key, and the cipher text document.

28. An encryption system for shared documents, comprising:

an encryption server system and a client system;

the encryption server system,

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

requesting the cipher text document from the server;

under control of the encryption server system,

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

29. An encryption system for shared documents, comprising:

an encryption server system and a client system;

under control of the encryption server system,

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

inserting the Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

under control of the client system,

requesting the clear text document from the server;

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document.

30. An encryption system for shared documents, comprising:

an encryption server system and a client system;

the encryption server system,

generating a ECC public/private key pair for the encryption server system;

transmitting the Java® encryption applet to the client system over a secure channel;

transmitting the encryption server system EEC public key to the client system over a secure channel;

storing the cipher text document in a storage medium;

storing the encrypted Triple DES symmetric key in a storage medium;

storing the relationship created between the cipher text document and the encrypted Triple DES symmetric key in a storage medium;

using the first entry in the correlation table to retrieve the encrypted Triple DES symmetric key;

decrypting the Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

inserting the encrypted Triple DES symmetric key into a Java® decryption applet;

sending the Java® decryption applet to the client system over a secure channel;

sending the cipher text document to the client system;

decrypting the encrypted Triple DES symmetric key using the encryption server system EEC private key, thereby creating a decrypted Triple DES symmetric key;

sending the cipher text document to the client system;

generating a Triple DES symmetric key;

encrypting the clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

a client system,

requesting a Java® encryption applet from the encryption server system;

requesting an encryption server system EEC public key from the encryption server system;

receiving the Java® encryption applet from encryption server system over a secure connection;

receiving an encryption server system EEC public key from the encryption server system over a secure channel;

installing the Java® encryption applet on the client system;

running the Java® encryption applet on the client system to generate a Triple DES symmetric key;

encrypting a clear text document with the Triple DES symmetric key, thereby creating a cipher text document;

creating a relationship between the cipher text document and the Triple DES symmetric key;

encrypting Triple DES symmetric key with the encryption server EEC public key, thereby creating an encrypted Triple DES symmetric key;

creating a relationship between the cipher text document and the encrypted Triple DES symmetric key;

transmitting the document encrypted with the Triple DES symmetric key from the client system to the encryption server system;

transmitting the Triple DES symmetric key encrypted with the encryption server system EEC public key from the client system to the encryption server system;

transmitting the relationship between the cipher text document and the encrypted Triple DES symmetric key to the encryption server system;

requesting the cipher text document from the server;

installing the Java® decryption applet on the client system; and,

decrypting the cipher text document using the Java® decryption applet, thereby creating a clear text document; and,

requesting the clear text document from the server.